

Amendment to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claim 1 (currently amended): A method for providing a first service and a second service to a user via a client being coupled to a data communication network, said first service being provided by a first network server also being coupled to the data communication network, said second service being provided by a second network server also being coupled to the data communication network, said method comprising:

receiving a first request from the first network server to provide the first service to the user;

storing first data on the client in response to the received first request, said first data identifying the first service wherein authentication of the user by the first service is optional; allowing the user to access the first service without authenticating the user;

receiving a second request from the second network server to provide the second service to the user wherein the second service requires authentication of the user;

allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request; and

wherein, in response to ~~allowing the authentication of the user access by the second service request~~, the user is ~~allowed access to~~ authenticated for the first service as a result of the stored first data.

Claim 2 (original): The method of claim 1, wherein the first service and the second service are in different domains.

Claim 3 (original): The method of claim 1, wherein the stored first data indicates a policy group associated with the first service, and further comprising allowing, in response to allowing the user access to the second service, the user access to the first service if the second service is associated with the policy group indicated by the stored first data.

Claim 4 (original): The method of claim 3, wherein members of the policy group share a set of business rules, said set of business rules comprising a privacy policy.

Claim 5 (original): The method of claim 1, wherein said first request indicates a desire of the first network server to provide the first service to the user, and wherein said receiving the first request comprises receiving the first request from a first network server via an image tag.

Claim 6 (original): The method of claim 1, further comprising storing second data on the client in response to the received first request, said second data being issued by the first network server to indicate that the first network server has requested to provide the first service to the user.

Claim 7 (original): The method of claim 6, wherein the first data and the second data are implemented as cookies stored on the client.

Claim 8 (original): The method of claim 6, wherein on a subsequent visit to the first network server by the user, the first network server is adapted not to request to provide the first service to the user if the second data is stored on the client.

Claim 9 (original): The method of claim 6, wherein the stored first data indicates a policy group associated with the first service, and further comprising deleting the second data from the client in response to allowing the user access to the second service if the second service is associated with the policy group indicated by the stored first data.

Claim 10 (original): The method of claim 9, wherein said deleting comprises rendering a web page to the client, said web page including an image tag directing the client to a script of the second service, said script adapted to delete the second data from the client.

Claim 11 (canceled).

Claim 12 (currently amended): The method of claim [[1]]1, further comprising generating an authentication ticket and communicating the generated authentication ticket to the second network server after the user has been authenticated.

Claim 13 (original): The method of claim 12, further comprising:
communicating the generated authentication ticket to the first network server in response to deleting the second data from the client; and
wherein the user is authenticated for access to the first service as a result of the generated authentication ticket being communicated to the first network server.

Claim 14 (canceled).

Claim 15 (currently amended): A method for providing a first service and a second service to a user via a client being coupled to a data communication network, said first service being provided by a first network server also being coupled to the data communication network, said second service being provided by a second network server also being coupled to the data communication network, said method comprising:

receiving a first request from the first network server to provide the first service to the user wherein the first service requires authentication of the user;

authenticating the user for the first service in response to the received first request;

allowing the user access to the first service in response to the received first request;

storing first data on the client in response to allowing the user access to the first service, said first data identifying a first policy group associated with the first service, said first policy group having a shared set of business rules to restrict authentication of a user across different domains;

receiving a second request from the second network server to provide the second service to the user wherein authentication of the user by the second service is optional;

if the second service is associated with the first policy group identified by the stored first data, allowing the user access to the second service in response to the received second request wherein the user is authenticated for the second service in response to the received second request; and

if the second service is not associated with the first policy group identified by the stored first data[.];

updating the stored first data to identify the second service; and
allowing the unauthenticated user to access the second service.

Claims 16-18 (canceled).

Claim 19 (original): The method of claim 15, wherein the updated first data further identifies a second policy group associated with the second service.

Claim 20 (original): The method of claim 19, further comprising:
receiving a third request from a third network server to provide a third service to the user, said third network server also being coupled to the data communication network;
authenticating the user for access to the third service in response to the received third request;
allowing the user access to the third service if the user has been authenticated; and
wherein, in response to allowing the user access to the third service, the user is allowed access to the second service on a subsequent visit to the second network server if the third service is associated with the second policy group identified by the updated first data.

Claim 21 (canceled).

Claim 22 (currently amended): A system for providing services to a user, said system comprising:

a first network server coupled to a data communication network, said first network server being configured to provide a first service to a user via a client also coupled to the data communication network;

a second network server coupled to the data communication network, said second network server being configured to provide a second service to the user via the client;

a central server coupled to the data communication network, said central server being configured to receive a first request from the first network server to provide the first service to

the user and a second request from the second network server to provide the second service to the user;

said first network server being configured to direct the first request to the central server, said central server further being configured to generate and store first data on the client in response to receiving the first request, said first data identifying the first service wherein authentication of the user by the first service is optional;

said second network server being configured to direct the second request to the central server, said second service requires authentication of the user;

wherein, in response to the received second request, the central server is configured to allow the user access to the second service wherein the user is authenticated for the second service in response to the received second request; and

wherein, in response to authentication of ~~allowing~~ the user ~~access to~~ by the second ~~service request~~, the central server is configured to authenticate ~~allow~~ the user ~~access to~~ for the first service as a result of the stored first data.

Claim 23 (original): The system of claim 22, wherein the first network server and the second network server are configured to communicate the first request and the second request to the central server via an image tag, and wherein the first request indicates a desire of the first network server to provide the first service to the user.

Claim 24-29 (canceled).

Claim 30 (currently amended): A system for providing services to a user, said system comprising:

a first network server coupled to a data communication network, said first network server being configured to provide a first service to a user via a client also coupled to the data communication network, said first service requiring authentication of the user;

a second network server coupled to the data communication network, said second network server being configured to provide a second service to the user via the client, wherein the authentication of the user by said second service is optional;

a central server coupled to the data communication network, said central server being configured to receive a first request from the first network server to provide the first service to the user and a second request from the second network server to provide the second service to the user;

a database associated with the central server, said database being configured to store information identifying a first policy group associated with the first service and a second policy group associated with the second service, wherein the first policy group defines a shared set of business rules to restrict authentication of a user across different domains and the second policy group defines a shared set of business rules to restrict authentication of a user across different domains;

wherein, in response to the received first request, the central server is configured to allow the user access to the first service and to generate and store first data on the client based on the stored information identifying the first policy group associated with the first service, said first data identifying the first policy group associated with the first service wherein the central server authenticates the user for the first service in response to the received first request;

wherein if the second policy group identified by the stored information identifying the second policy group associated with the second service is the same as the first policy group identified by the stored first data, the central server is configured to allow the user access to the second service in response to the received second request wherein the user is authenticated by the central server for the second service in response to the received second request; and

wherein if the second policy group identified by the stored information identifying the second policy group associated with the second service is not the same as the first policy group identified by the stored first data, the central server is configured to update the stored first data to identify the second service in response to the received second request and the central server is configured to allow the unauthenticated user to access the second service.

Claim 31 (canceled).

Claim 32 (currently amended): The system of claim 30, wherein the second network server is being configured to generate and store second data on the client if the second policy group identified by the stored information identifying the second policy group associated with

the second service is not the same as the first policy group identified by the stored first data, said second data indicating that the second network server has communicated the second request to the central server, said second request indicating a desire of the second network server to provide the second service to the user; and

wherein on a subsequent visit to the second network server by the user, the second network server is configured not to direct a request to the central server to provide the second service to the user if the second data is stored on the client.

Claim 33 (original): The system of claim 30, wherein the updated first data further identifies the second policy group associated with the second service.

Claim 34 (currently amended): The system of claim 33, further comprising:

a third network server coupled to the data communication network, said third network server being configured to provide a third service to the user via the client;

said central server being further configured to receive a third request from the third network server to provide the third service to the user and to authenticate the user for access to the third service in response to the received third request;

wherein the stored information identifying the third policy group associated with the third service further identifies a third policy group associated with the third service, the third policy group defines a shared set of business rules to restrict authentication of a user across different domains; and

wherein the central server is configured to allow the user access to the second service on a subsequent visit to the second network server if the user has been authenticated and if the third policy group identified by the stored information identifying the third policy group associated with the third service is the same as the second policy group identified by the updated first data.

Claim 35 (currently amended): One or more computer-readable media having computer-executable components for providing a first service and a second service to a user via a client being coupled to a data communication network, said first service being provided by a first network server also being coupled to the data communication network, said second service being

provided by a second network server also being coupled to the data communication network, said computer-readable media comprising:

a redirect component for receiving a first request from the first network server to provide the first service to the user and for receiving a second request from the second network server to provide the second service to the user;

a response component for storing first data on the client in response to the received first request, said first data identifying the first service wherein authentication of the user by the first service is optional;

an authentication component for allowing the user access to the second service in response to the received second request wherein the second service requires authentication of the user and the user is authenticated for the second service in response to the received second request; and

wherein, in response to ~~allowing the authentication of the user access to~~ allow authenticate the user ~~access to~~ for the first service as a result of the stored first data.

Claim 36 (original): The computer-readable media of claim 35, further comprising a storage component for storing information identifying a policy group associated with the second service, wherein the stored first data indicates a policy group associated with the first service, and wherein, in response to allowing the user access to the second service, the authentication component is adapted to allow the user access to the first service if the policy group identified by the stored information is the same as the policy group indicated by the stored first data.

Claim 37 (original): The computer-readable media of claim 35, wherein the first request indicates a desire of the first network server to provide the first service to the user, wherein the response component is adapted to store second data on the client in response to the received first request, said second data indicating that the first network server has requested to provide the first service to the user, and wherein on a subsequent visit to the first network server by the user, the first network server is adapted not to request to provide the first service to the user if the second data is stored on the client.

Claim 38 (original): The computer-readable media of claim 37, further comprising:
a storage component for storing information identifying a policy group associated with the second service;

wherein the stored first data indicates a policy group associated with the first service; and
wherein, in response to allowing the user access to the second service, if the policy group identified by the stored information is the same as the policy group indicated by the stored first data, the response component is adapted to render a web page to the client, said web page including an image tag directing to a script of the second service, said script adapted to delete the second data from the client.

Claim 39-40 (canceled).